AMENDMENTS TO THE CLAIMS

1. (Currently Amended) A method of authenticating a user identity module implemented in an access terminal, comprising:

receiving, at the access terminal and over an air interface, a first challenge associated with a first authentication process;

deriving, at the access terminal, a second challenge associated with a second authentication process based on at least a portion of the first challenge;

performing, at the user identity module, the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom; and

deriving, at the access terminal, a key associated with the first authentication process based on the at least one authentication parameter.

2. (Original) A method, as set forth in claim 1, wherein receiving the first challenge associated with the first authentication process further comprises receiving a CHAP challenge.

3. (Original) A method, as set forth in claim 2, wherein deriving the second challenge associated with the second authentication process based on at least a portion of the first challenge further comprises deriving a RAND challenge based on at least a portion of the CHAP challenge.

4. (Currently Amended) A method, as set forth in claim 3, wherein deriving the RAND challenge based on at least a portion of the CHAP challenge further comprises deriving the RAND challenge from a selected number of least significant bits in ~~by concatenating~~ the CHAP challenge.

5. (Original) A method, as set forth in claim 4, wherein performing the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom further comprises performing a CAVE based authentication process on the RAND challenge to produce SMEKEY.

6. (Original) A method, as set forth in claim 5 wherein performing the CAVE based authentication process on the RAND challenge to produce SMEKEY further comprises performing the CAVE based authentication process on the RAND challenge to produce SMEKEY and PLCM.

7. (Original) A method, as set forth in claim 6, wherein deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises deriving the key associated with the first authentication process based on SMEKEY and PLCM.

8. (Currently Amended) A method, as set forth in claim 1, further comprising:

generating, at the access terminal, an authentication response based on the key; and

delivering the [[key]] authentication response over the air interface to a network to request access to the network.

9. (Original) A method, as set forth in claim 8, further comprising:

determining that the first challenge associated with the first authentication process is a re-authentication challenge;

bypassing the derivation of the second challenge associated with the second authentication process based on at least a portion of the first challenge in response to the determining that the first challenge is the re-authentication challenge;

bypassing the performance of the second authentication process using the derived second challenge and producing at least one authentication parameter therefrom in response to the determining that the first challenge is the re-authentication challenge; and wherein

deriving the key associated with the first authentication process based on the at least one authentication parameter further comprises using a previously derived key in response to the determining that the first challenge is the re-authentication challenge.

10. (Original) A method, as set forth in claim 8, further comprising:

determining that the first challenge associated with the first authentication process is a re-authentication challenge; and wherein

delivering the key to a network to request access to the network further comprises delivering a previously derived key in response to the determining that the first challenge is the re-authentication challenge.

11. (Original) A method, comprising:

receiving a CHAP challenge;

deriving a RAND challenge based on at least a portion of the CHAP challenge;

performing an authentication using the RAND challenge to produce a SMEKEY and a PLCM; and

deriving a secret CHAP key based on the SMEKEY and PLCM.